THE EVENING STAR DATE 16 OCT 70 PAGE 2

Laird Eases Release Of Technical Papers

The Pentagon is stripping security classifications from thousands of technical documents in an effort to make more information available to the general public and the technical community.

Defense Secretary Melvin R. Laird announced what was described as a "major policy change" yesterday. Under the new policy, security classifications such as secret and top secret will be assigned to documents only after study of two considerations, Laird said.

In the past, his announcement said, the major consideration for restricting data has been the possible benefit of the information to potential enemies.

Now, major consideration in favor of disclosure will be given to the possible benefits to the United States and its allies through the use of the information.

The new policy will sharply cut back on the number of both classified and unclassified documents whose distribution is limited.

Each year about 45,000 defense technical documents are prepared. Of these, about 17 percent are withheld from public distribution for security reasons. Another 39 percent are limited in their distribution.

In the past, documents could be marked "no foreign," "U.S. Government only," or "Department of Defense only," and marked for use of certain individuals.

Now, the only such restriction will be "U.S. government only." This will be used to protect information given to this government by other countries or by private businesses with some restriction on its distribution.

Although the new rules have been ordered by Laird, the restrictions previously pleaded on documents will be allowed to expire normally. They usually run three years. In addition, there will be a review of documents classified for security reasons, to be completed by Jan. 1, 1972.

As an example of the change in policy, a report of the National Materials Advisory Board on "Hot Corrosion in Gas Turbines" has long been restricted and could not be given to foreign governments or foreign nationals.

This morning, an advisory board official called the Pentagon and asked if the document now can be made available for unlimited distribution. It was, within a few minutes, and a sticker was pasted to the report: "This document has been approved for public release. It's distribution is unlimited."

in full. This includes physician services, psychiatric services, hospital and other institutional care, dental services, medicines, therapeutic devices, appliances, and equipment, as well as needed supporting services.

Furthermore, money will be provided to develop a more adequate supply and appropriate distribution of health professionals and supporting personnel. The program will actively encourage more efficient organization of existing health manpower, provide funds for special training of physicians, dentists, and other health workers needed for this program, and apply financial incentives to stimulate the movement of health manpower to medically deprived areas.

We have heard talk all during this Congress that there were "new" proposals forthcoming from the administration, that we should wait and see.

Mr. President, I have been urged for months to wait and see, that the administration will have a bill. And I have been waiting. But it is late in the session. The time for waiting is now past. We can no longer wait for a band-aid approach for our disintegrating health system that needs major surgery. While the bill I introduce today is not the complete answer, it is the best answer we have yet come up with.

Mr. President, I have been on the Health Subcommittee of the Senate for nearly 13 years, up until last year under the great Lister Hill as chairman. I have listened to the evidence for 13 years. We have talked to the experts, and we have studied this question for years. Last January, when I became chairman of the subcommittee, I expressed a desire to introduce such a comprehensive health care bill. This, I repeat, is the best we have been able to come up with after hearing testimony from the people who have worked in this field over in the private structure of the economy, made a study of the problem, and come in with their recommendations.

I ask unanimous consent that the bill be printed in the RECORD.

The PRESIDING OFFICER (Mr. BELLMON). The bill will be received and appropriately referred; and, without objection, the bill will be printed in the RECORD in accordance with the Senator's request.

The bill (S. 4323) to create a health security program, introduced by Mr. YARBOROUGH (for himself, Mr. KENNEDY, Mr. COOPER, and Mr. SAXBE), was received, read twice by its title, referred to the Committee on Labor and Public Welfare, and ordered to be printed in the RECORD, as follows:

[The bill will be printed in a subsequent edition of the RECORD.]

ADDITIONAL COSPONSOR OF A BILL

S. 3220

At the request of the Senator from West Virginia (Mr. BYRD) the Senator from Nevada (Mr. CANNON) was added as a cosponsor of S. 3220, to protect a person's right of privacy by providing for the designation of obscene or offensive mail matter by the sender and for the return of such matter at the expense of the sender.

CORRECTION OF ANNOUNCEMENT ON VOTE

Mr. GRIFFIN. Mr. President, on behalf of the Senator from Colorado (Mr. ALLOTT), I ask that the permanent RECORD be corrected to show that on vote No. 283, the passage of the Treasury-Post Office appropriation bill for 1971, the Senator from Colorado, if present and voting, would have voted "yea."

PROPOSED AMENDMENT TO THE CONSTITUTION RELATING TO DIRECT POPULAR ELECTION OF THE PRESIDENT AND VICE PRESIDENT—AMENDMENTS

AMENDMENT NO. 878

Mr. GRIFFIN submitted amendments, intended to be proposed by him, to the joint resolution (S.J. Res. 1) proposing an amendment to the Constitution to provide for the direct popular election of the President and Vice President of the United States, which were ordered to lie on the table and to be printed.

ANNOUNCEMENT OF HEARINGS: FEDERAL DATA BANKS AND THE BILL OF RIGHTS

Mr. ERVIN. Mr. President, in recent months, with the discovery of each new Federal data bank and data system, public concern has increased that some of the Federal Government's collection, storage, and use of information about citizens may raise serious questions of individual privacy and constitutional rights.

The Constitutional Rights Subcommittee has received countless letters and telegrams from Members of Congress and from interested persons all over the United States, urging that hearings be scheduled to consider the total impact of some of these data programs on preservation of individual rights.

I wish to announce that, in response to these demands, the subcommittee has scheduled a new series of hearings on "Federal data banks and systems and the bill of rights." The first stage of the hearings will be held October 6, 7, and 8.

The subcommittee has already undertaken a survey of Federal data banks and automated data systems to determine what statutory and administrative controls are governing their growth and what rights and remedies are provided for the citizen. The analysis of the executive branch replies to that subcommittee questionnaire, together with the hearings held in the last session on "privacy and Federal questionnaires," and the hearings which begin in October, will assist Congress in determining the need for a new independent agency to control Federal data banks on behalf of the privacy and due process rights of citizens. It has been my conviction that such an agency is needed, along with new remedies in the courts and other corrective actions. I detailed the reasons for my belief in a Senate speech in November 1969.

The purpose of the hearings is: First, to learn what Government data banks have been developed; second, how far they are already computerized or automated; third, what constitutional rights, if any, are affected by them; and, fourth, what overall legislative controls, if any, are required.

Witnesses familiar with the constitutional and legal issues, as well as the practical problems raised by some current and proposed data programs will document these for the record. The Secretary of the Army and other representatives of the Defense Department have already been invited to attend the October hearings to describe how and why the Army and other armed services have collected and stored information on civilians, and to what extent the records have been automated for easy access and retrieval.

Prof. Arthur R. Miller of the University of Michigan Law School, author of a forthcoming book, "The Dossier Society: Personal Privacy in the Computer Age," has been invited to describe the state of the law governing information flow in our society and its relationship to legal rights. Another witness will be Christopher Pyle, an attorney and former Army intelligence officer, who has investigated the Army's civil disturbance data programs, and has written widely on the subject.

In later hearings, other representatives of the executive departments and agencies will be invited to respond to the complaints and fears which have been expressed by the public. They will be afforded the opportunity to explain exactly what their data programs on people involve, and how, if at all, the privacy, confidentiality and due process rights of the individual are respected.

The subcommittee has received enthusiastic support from specialists in the computer sciences, in both the computer industry and in the academic community. We hope to receive the benefit of their expertise for our hearing record.

Mr. President, our Nation is predicated on the fundamental proposition that citizens have a right to express their views on the wisdom and course of governmental policies. This involves more than the currently popular notion of a so-called right to dissent. Our system cannot survive if citizen participation is limited merely to registering disagreement with official policy; the policies themselves must be the product of the people's views. The protection and encouragement of such participation is a principal purpose of the first amendment.

More than at any other time in our history, people are actively expressing themselves on public questions and seeking to participate more directly in the formulation of policy. Mass media have made it easy for large numbers of people to organize and express their views in written and oral fashion. Rapid means of transportation have aided our mobile population to move easily to sites of central and local authority for the purpose

of expressing their views more publicly. The freedom of our form of government and the richness of our economy have made it possible for individuals to move about freely and to seek their best interests as they will in vocations and avocations of their choice, or indeed, to pursue none at all for a time, if that is what they wish. If modern technology has provided citizens with more efficient means for recording their dissent, or for registering their political, economic, or social views, it has also placed in the hands of executive branch officials new methods of taking note of that expression of views and that political activity. For these reasons, those individuals who work actively for public causes are more visible than ever before.

These new sciences have accorded those who control government increased power to discover and record immutably the activities, thoughts and philosophy of an individual at any given moment of his life. That picture of the person is recorded forever, no matter how the person may change as time goes on. Every person's past thus becomes an inescapable part of his present and future. The computer never forgets.

To be sure, recordkeeping is nothing new in the history of government; nor indeed, is the habit all governments and all societies have of surveillance, blacklisting and subtle reprisal for unpopular political or social views. Men have always had to contend with the memories of other men. In the United States, however, we are blessed with a Constitution which provides for due process of law. This applies to the arbitrary use of the recordkeeping and information power of government against the individual.

Despite these guarantees, the new technology has been quietly, but steadily, endowing officials with the unprecedented political power which accompanies computers and data banks and scientific techniques of managing information. It has given Government the power to take note of anything, whether it be right or wrong, relevant to any purpose or not, and to retain it forever. Unfortunately, this revolution is coming about under outdated laws and executive orders governing the recordkeeping and the concepts of privacy and confidentiality relevant to an earlier time.

These developments are particularly significant in their effect on the first amendment to our Constitution.

No longer can a man march with a sign down Pennsylvania Avenue and then return to his hometown, his identity forgotten, if not his cause.

No longer does the memory of the authorship of a political article fade as the pages of his rhetoric yellow and crumble with time.

No longer are the flambovant words exchanged in debate allowed to echo into the past and lose their relevance with the issue of the moment which prompted them.

No longer can a man be assured of his enjoyment of the harvest of wisdom and maturity which comes with age, when the indiscretions of youth, if noticed at all, are spread about in forgotten file cabinets in basement archives.

Instead, today, his activities are recorded in computers or data banks, or if not, they may well be a part of a great investigative index.

Some examples come readily to mind from the subcommittee survey.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2-120,000 index cards. These bear lead information relating to possible questions of suitability involving loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II. The Commission has found it a reasonable, economical and invaluable tool in meeting its investigative responsibilities. It is useful to all Federal agencies as an important source of information.

The Commission chairman reports:

> Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting.

In its "security investigations index," the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigations made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

The Commission's "investigative file" consists of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

For authorization for these data banks, the Commission cites Executive Order 10450, an order promulgated in 1953.

Another department, the Housing and Urban Development Department, is considering automation of a departmental procedure. According to the report made to the subcommittee:

> The data base would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File. A data bank consisting of approximately 325,000 3x5 index cards has been prepared covering any individual or firm which was the subject of, or mentioned prominently in any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well. In addition, HUD maintains an index file on all Department employees which reflects dates and types of personnel security investigations conducted under the provisions of Executive Order 10450.

In the interest of preparing for possible civil disturbances and for protecting the armed services from subversion, the Department of the Army and other military departments have been collecting information about civilians who have no dealing with the military services.

The Secret Service has created a computerized data bank in the pursuit of its programs to protect high Government officials from harm and Federal buildings from damage. Their guidelines for inclusion of citizens in this data bank refer to "information on professional gate crashers; information regarding civil disturbances; information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas; information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, and so forth."

In the area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs. The initial data base, according to the Secretary of the Treasury, is a "modest" one comprising some 3,000 suspect records: He states:

> These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and usable form. With the coordinated efforts of the Agency Service's intelligence activities, steady growth of the suspect files is expected.

This data bank, which is used by the Bureau to identify suspect persons and vehicles entering the United States, is an "essential tool" in performance of Customs officers' search and seizure authority, Secretary Kennedy has stated.

The Department of Justice is establishing comprehensive law enforcement data systems in cooperation with State governments, and is funding State data programs for law enforcement, civil disturbance and other surveillance purposes.

The National Science Foundation has created a data bank of scientists.

The Department of Health, Education, and Welfare has established a data bank on migrant children to facilitate the transfer of school records.

During our subcommittee hearings last year, case after case was documented of the vast programs to coerce citizens into supplying personal information for statistical data banks in the Census Bureau and throughout other Federal agencies.

These are only a few of the data programs which have raised due process of law questions from Congress and the public.

How do these things come about? It would be unfair, perhaps, to attribute suspicious political motives, or lack of ethics to those responsible for any one program or for any group of programs for collecting and storing personal information about citizens. Frequently, they just grow over the years. Sometimes, executive department data banks are either merely good faith efforts at fulfillment of specific mandates from Congress; or they are based on what some of-

ficials think to be implied mandates to acquire information necessary for Congress to legislate. If so, then Congress has no one to blame but itself when such programs unnecessarily threaten privacy or other rights. But it then has an even greater responsibility for acting, once its own negligence is discovered.

Perhaps the most such officials can be charged with is overzealousness in doing their job within narrow confines, to the exclusion of all other considerations.

Sometimes the issue of threats to individual rights is presented only after a data system has developed, and only after practical problems are raised which were not envisioned on paper.

At times, due process may be threatened by the failure of the computer specialists to consider only the information on a person absolutely essential for their programing.

There are political reasons also. One is the failure of heads of executive departments and agencies to mind their own stores and stay out of the business of other agencies. Each department does not not need to seize the total man when it administers a program; only those portions of him necessary for the job. Another reason is the tendency of executive branch officials in the interest of political expediency and shortcuts to law and order goals, to seize upon the techniques of data banks, intelligence gathering, and surveillance activities as a substitute for hard-hitting, practical law enforcement work by the proper agencies, and for creative administration of the laws.

All of these excuses will not help the law-abiding citizen who, at the whim of some official, is put into an intelligence-type data bank which is part of a network of inquiry for all manner of governmental purposes.

No one would deny that the Government of such a populous and farflung country should not avail itself of the efficiency offered by computers and scientific data management techniques. Clearly, Government agencies must, as Congress has charged them, acquire, store, and process economically the information it obtains from citizens for administrative purposes. There is an ever-increasing need for information of all kinds to enable the Congress to legislate effectively and the executive branch to administer the laws properly.

Furthermore, there is an obvious need in such a complex mobile society for recording and documenting amply the official relationship between the individual and his government.

More and more frequently, misguided individuals are resorting to violence and violation of the law. Communities are faced with rising crime rates. Local, State, and Federal Government have a right and a duty to know when a person has a legal record of violation of the law which, under the law, would deny him certain rights or benefits. They should be able to ascertain these matters quickly.

There are always some problems of accuracy and confidentiality with such records, especially when automated. It is not the carefully designed individual law enforcement data banks which concern the public. Rather, the subcommittee study is revealing that data programs which have aroused the most apprehension recently are those—

Which bear on the quality of first amendment freedoms by prying into those protected areas of an individual's personality, life, habits, beliefs, and legal activities which should be none of the business of Government even in good causes;

Which are unauthorized, or unwarranted for the legitimate purpose of the agency;

Which keep the information they acquire too long, and which by the very retention of unknown data may intimidate the individual subject;

Which are part of a network of data systems;

Which make little, if any provision for assuring due process for the individual in terms of accuracy, fairness, review, and proper use of data, and thereby may operate to deny the individual rights, benefits, privileges, reputation, which are within the power of government to influence, grant or deny.

There is growing concern that the zeal of computer technicians, of the systems planners, and of the political administrators in charge of the data systems threatens to curtail the forces of society which have operated throughout our history to cool political passions and to make our form of government viable by allowing a free exchange in the marketplace of ideas.

The new technology has made it literally impossible for a man to start again in our society. It has removed the quality of mercy from our institutions by making it impossible to forget, to forgive, to understand, to tolerate. When it is used to intimidate and to inhibit the individual in his freedom of movement, associations, or expression of ideas within the law, the new technology provides the means for the worst sort of tyranny. Those who so misuse it to augment their own power break faith with those founders of our Constitution who, like Thomas Jefferson, swore upon the altar of God eternal hostility against every form of tyranny over the mind of man.

Mr. President, it has become dangerously clear in recent times that unless new controls are enacted, new legal remedies are provided, and unless Federal officials can be persuaded to exercise more political self-control, this country will not reap the blessings of man's creative spirit which is reflected in computed technology. Rather, if the surveilliance it encourages is allowed to continue without strict controls and safeguards, we stand to lose the spiritual and intellectual liberty of the individual which have been so carefully nourished and so valianty defended, and which our Founding Fathers so meticulously enshrined in the Constitution.

I say this out of my conviction that the undisputed and unlimited possession of the resources to build and operate data banks on individuals, and to make decisions about people with the aid of computers and electronic data systems, is fast securing to executive branch officials a political power which the authors of the Constitution never meant any one group of men to have over all others. It threatens to unsettle forever the balance of power established by our Federal Constitution.

Our form of government is the fruition of an ideal of political, economic, and spiritual freedom which is firmly rooted in our historical experience. Basic to its fulfillment has always been the monumental truth that such freedom is truly secure only when power is divided, limited, and called to account by the people. For this reason the central Government was divided into three separate and equal branches.

For this reason, the bill of rights was added to secure certain areas of liberty against incursion by Government and the exercise of Federal power was limited to certain purposes.

For this reason, we cherish and protect the legal freedom of each citizen to develop his mind and personality and to express them free of unwarranted governmental control.

I differ with those who say that there are no existing checks on this developing power of computer technology, for I believe they already exist in our form of Government. The guarantees are established in our Constitution.

The forthcoming hearings will help Congress determine how these guarantees may best be implemented to meet the demands of the computer age.

In the interest of responding to the many inquiries from scholars, reporters and members of the public who are working on this subject, I should like to refer to other sources of materials which provide useful background information.

The subject of how Government manages its information systems, and its paperwork, how and when it uses computers and automation to assist in this effort, has been a continuing subject of concern by a number of congressional committees and their efforts should interest those working on this subject.

The Senate Administrative Practice and Procedures Subcommittee has contributed valuable hearings, reports and studies on the subject of computers, privacy, and Government dossiers. Particularly informative is their 1967 report "Government Dossier: Survey of Information on Individuals Contained in Government Files."

The Senate Government Operations Committee has, in other years, conducted comprehensive hearings and issued reports on Government information systems and management uses of computers.

In the House of Representatives, the Committee on Science and Astronautics has held a provocative and stimulating series of hearings and panel discussions on the impact of technology, especially on the management of Government information.

The House Government Activities Subcommittee of the Government Operations Committee, chaired by Representative JACK BROOKS, has produced valuable hearings, reports and legislation on "Data Processing Management in the Federal Government."

More than anyone else, Representative CORNELIUS GALLAGHER has continu-

ally pointed out the dangers to individual rights and privacy of the establishment of a national data center, and his Special Subcommittee on Invasion of Privacy, after stimulating hearings, produced a classic and concise report entitled, "The Data Bank Concept." The record of his hearings contains testimony from many expert witnesses on the philosophy of privacy and computer technology.

The Census and Statistics Subcommittee of the House Post Office and Civil Service Committee produced a thought-provoking and influential report in the 89th Congress entitled "The Federal Paperwork Jungle." Scholars will find most informative that subcommittee's hearings and reports dealing with the paperwork requirements placed upon business, industry, and the public by the Federal departments.

I commend the publications of all of these committees and the thoughtful speeches of the chairmen and the members of these committees to persons interested in this subject.

It is my hope that the hearings and study by the Constitutional Rights Subcommittee will add a unique and valuable dimension to the public and congressional dialog on the role of data banks, information systems, and computers in our constitutional form of government.

Ben A. Franklin, in an excellent article in the New York Times on June 28, 1970, has described some of the current data banks and computers in the Federal Government and their possible effect on individual rights and privacy. I ask unanimous consent that his most perceptive article be printed in the RECORD at this point together with the following thoughtful articles and editorials. These are only a few of the excellent editorials and articles on this subject which have come to my attention, and they suggest a nationwide interest.

Editorials from the Greensboro, N.C., Daily News, July 1, 1970; Asheville, N.C., Times, June 18, 1970; Omaha, Nebr., World Herald, January 15, 1970; Sioux Falls, S. Dak., Argus, January 16, 1970; New York Post, June 30, 1970; Washington, D.C., Post, April 24, 1970; Asheville, N.C., Citizen, July 2, 1970; New York Times, July 4, 1970; Computerworld, March 4, 1970, and August 27, 1969; Huntsville, Ala., Times, July 12, 1970; Washington, D.C., Evening Star, March 16, 1970; and Houston, Tex., Post, March 16, 1970.

An article by Tom Wicker, entitled "In the Nation: A Right Not To Be Data-Banked?" from the New York Times, July 7, 1970, and an article from the Boston, Mass., Herald Traveler by John S. Lang, entitled "Big Brother, U.S., Is Watching You," April 19, 1970, an article from the Morning Call, Allentown, Pa., entitled "Guardian of Freedom," June 30, 1970, "Mitchell Defends Justice Department's 'Big Brother' Role," by Jared Stout Staten Island, N.Y., Advance, July 19, 1970, and "Justice Department Keeps Files on Activists," by Morton Kondracke, Roanoke, Va., World News, March 11, 1970.

There being no objection, the editorials and articles were ordered to be printed in the RECORD, as follows:

[From the New York Times, June 28, 1970]

FEDERAL COMPUTERS AMASS FILES ON SUSPECT CITIZENS—MANY AMONG HUNDREDS OF THOUSANDS LISTED HAVE NO CRIMINAL RECORDS—CRITICS SEE INVASION OF PRIVACY

(By Ben A. Franklin)

WASHINGTON, June 27.—The police, security and military intelligence agencies of the Federal Government are quietly compiling a mass of computerized and microfilmed files here on hundreds of thousands of law abiding yet suspect Americans.

With the justification that a revolutionary age of assassination, violent political dissent and civil disorder requires it, the Government is building an army of instantly retrievable information on "persons of interest."

The phrase is an agent's term for those citizens, many with no criminal records, whom the Government wants to keep track of in an effort to avert subversion, rioting and violence or harm to the nation's leaders.

Critics of this surveillance, so far few in number, believe that the collection and dissemination of such information on noncriminals—for whatever purpose—is unauthorized by law and raises the most serious constitutional questions.

The foremost among them, Senator Sam J. Ervin, Jr., Democrat of North Carolina, has said that computerized files already in existence here are leading the country toward a "police state."

Discussions with officials, an examination of some known data files and information supplied by the Senator show that the files often contain seemingly localized and mundane information, reflecting events that today are virtually commonplace.

The leader of a Negro protest against welfare regulations in St. Louis, for example, is the subject of a teletyped "spot report" to Washington shared by as many as half a dozen Government intelligence gathering groups.

The name of a college professor who finds himself unwittingly, even innocently, arrested for disorderly conduct in a police roundup at a peace rally in San Francisco goes into the data file.

A student fight in an Alabama high school is recorded—if it is interracial.

Government officials insist that the information is needed and is handled discreetly to protect the innocent, the minor offender and the repentant.

The critics—including the Washington chapter of the American Civil Liberties Union and Representative Cornelius E. Gallagher, Democrat of New Jersey—charge that the system is an invasion of privacy and a potential infringement of First Amendment rights of free speech and assembly.

MASS SURVEILLANCE SYSTEMS

Senator Ervin, a conservative, a student of the Constitution, a former judge of the North Carolina Superior Court, and the chairman of the Senate Subcommittee on Constitutional Rights, says that the advent of computer technology in Government file keeping is pushing the country toward "a mass surveillance system unprecedented in American history."

In a recent series of Senate speeches, Mr. Ervin said that the danger was being masked by a failure of Americans to understand "the computer mystique' and by the undoubted sincerity and desire for "efficiency" of the data bank operations and planners.

The Government is gathering information on its citizens at the following places:

A Secret Service computer, one of the newest and most sophisticated in Government. In its memory the names and dossiers of activists, "malcontents," persistent seekers of redress, and those who would "embarrass" the President or other Government leaders are filed with those of potential assassins and persons convicted of "threats against the President."

A data bank compiled by the Justice Department's civil disturbance group. It produces a weekly printout of national tension points on racial, class and political issues and the individuals and groups involved in them. Intelligence on peace rallies, welfare protests and the like provide the "data base" against which the computer measures the mood of the nation and the militancy of its citizens. Judgments are made; subjects are listed as "radical" or "moderate."

A huge file of microfilmed intelligence reports, clippings and other materials on civilian activity maintained by the Army's Counterintelligence Analysis Division in Alexandria, Va. Its purpose is to help prepare deployment estimates for troop commands on alert to response to civil disturbances in 25 American cities. Army intelligence was ordered earlier this year to destroy a larger data bank and to stop assigning agents to "penetrate" peace groups and civil rights organizations. But complaints persist that both are being continued. Civilian officials of the Army say they "assume" they are not.

Computer files intended to catch criminal suspects—the oldest and most advanced type with the longest success record—maintained by the Federal Bureau of Investigation's National Crime Information Center and recently installed by the Customs Bureau. The crime information center's computer provides 40,000 instant, automatic teletype printouts each day on wanted persons and stolen property to 49 states and Canada and it also "talks" to 24 other computers operated by state and local police departments for themselves and a total of 2,500 police jurisdictions. The centers says its information is all "from the public record," based on local and Federal warrants and complaints, but the sum product is available only to the police.

A growing number of data banks on other kinds of human behavior, including, for example, a cumulative computer file on 300,000 children of migrant farm workers kept by the Department of Health, Education, and Welfare. The object is to speed the distribution of their scholastic records, including such teacher judgments as "negative attitude," to school districts with large itinerant student enrollments. There is no statutory control over distribution of the data by its local recipients—to prospective employers, for example.

WARNING BY ERVIN

Senator Ervin has warned: "Regardless of the purpose, regardless of the confidentiality, regardless of the harm to any one individual [that might occur if there were no computer files], the very existence of Government files on how people exercise First Amendment rights, how they think, speak, assemble and act in lawful pursuits, is a form of official psychological coercion to keep silent and to refrain from acting."

But despite his sounding of such alarms, Senator Ervin has noted that there is "unusual public and Congressional complacency." When he speaks on the Senate floor of "techniques for monitoring our opinions" and of "grave threats to our freedoms," the chamber is more often than not nearly empty. He has gained little Congressional support and scant attention outside the Congress.

Meanwhile, various official and high-level pressures on Government agencies to acquire computers and to advance their surveillance are producing results.

The pressures include a stern recommen-

dation for the broadest possible surveillance of "malcontents" and potential assassins by the Warren Commission, which investigated the assassination of President Kennedy. The commission's mandate is widely cited in the Government as the authority for citizen surveillance.

The commission, headed by former Chief Justice Earl Warren, disapproved as too narrow, the criteria for persons to be bought under "protective" surveillance proposed in 1964 by the Secret Service. The guidelines were "unduly restrictive," the commission declared, because they required evidence of "some manifestation of animus" by disgruntled and activist citizens before those persons could be brought under Secret Service surveillance as poential "threats to the President."

EVERY AVAILABLE RESOURCE

"It will require every available resource of the Government to devise a practical system which has any reasonable possibility of revealing such malcontents," the commission said.

The guideline was broadened. A computer was installed by the Secret Service last January. The commission's edict became a surveillance bench mark.

For surveillance of persons who may be involved in civil disturbances, the riots of 1967 and 1968 served the same purpose.

"The Warren Commission and the riots legitimized procedures which, I grant you, would have been unthinkable and, frankly, unattainable from Congress in a different climate," one official said. "There are obvious questions and dangers in what we are doing but I think events have shown it is legitimate," the official declined to be quoted by name.

Senator Ervin contends that in the "total recall," the permanence, the speed and the interconnection of Government data files there "rests a potential for control and intimidation that is alien to our form of Government and foreign to a society of free men." The integration of data banks, mixing criminal with noncriminal files, is already underway, according to his subcommittee.

INTEGRATION OF FILES

The subcommittee has been advised by the Department of Housing and Urban Development, for example, that its data systems planners have proposed to integrate on computer tape files concerning the following: the identities of 325,000 Federal Housing Administration loan applicants; the agency's own "adverse information file," the Justice Department's organized crime and rackets file, and F.B.I. computer data on "investigations of housing matters." The object, the Department said, is a unified data bank listing persons who may be ineligible to do business with H.U.D.

As another example of how computer data proliferates, the subcommittee cites a report it received from the Internal Revenue Service.

The I.R.S., with millions of tax returns to process, was one of the earliest agencies to computerize. It has also had a reputation as a bastion of discretion. The privacy of individual tax returns has been widely regarded as inviolate, to be overcome only by order of the President.

But the subcommittee has been told that the I.R.S. has "for many years" been selling to state tax departments—for $75 a reel—copies of magnetic tapes containing encoded personal income tax information. It is used to catch non-filers and evaders of state taxes.

The District of Columbia and 30 states bought copies of the I.R.S. computer/covering returns from their jurisdictions in 1969, the service has told the subcommittee. Each local jurisdiction was merely "requested" to alert its employes that the unauthorized disclosure of Federal tax data was punishable by a $1,000 fine.

FIREARMS DATA FOR SALE

The I.R.S. also sells at cost—apparently to anyone who asks—the copies of its data files of registrants under the various Federal firearms laws it enforces.

The Secret Service computer file is capable of instant, highly sophisticated sorting and retrieval of individuals by name, alias, locale, method of operation, affiliation, and even by physical appearance.

The agency's Honeywell 2200, with random access capability, makes it possible to detect, investigate and detain in advance "persons of interest" who might intend—or officials concede "they might not but we don't take chances"—to harass, harm or "embarrass" officials under its protection.

Unknown to most Americans, the names, movements, organizations and "characteristics" of tens of thousands of them—criminals and noncriminals—are being encoded in the Secret Service data center here.

The names of other thousands have been inserted in less specialized computers operated by the Justice Department and the F.B.I. Although the agencies insist that they do not, the computers can—and Senator Ervin stresses that no law says they may not—"talk" to each other, trading and comparing in seconds data that may then spread further across the nation.

The Secret Service can now query its computer and quickly be forewarned that, say, three of the 100 invited guests at a Presidential gathering in the White House Rose Garden are "persons of protective interest."

Under current Secret Service criteria, they may have been regarded by someone as the authors of reportedly angry or threatening or "embarrassing" statements about the President or the Government. The action taken by the Secret Service may range from special observation during "proximity to the President" to withdrawal of the invitation.

What constitutes a computer-worthy "threat" thus becomes important. The Secret Service asserts that it applies relatively easy-going and "sophisticated" standards in deciding who is to be encoded. But the critics point out that the vast capacity of a computer for names and dossiers—unlike that of a paper filing system, which has self-limiting ceiling based on the ability to retrieve—is an encouragement to growth.

The information or "data base" for a Secret Service computer name check flows into the protective intelligence division from many sources—abusive or threatening letters or telephone calls received at the White House, F.B.I. reports, military intelligence, the Central Intelligence Agency, local police departments, the Internal Revenue Service, Federal building guards, individual informants.

Much of it that may be "of interest" to the Federal monitors of civil disturbance data is screened out, Secret Service spokesmen say, or is merely name-indexed by the computer with a reference to data reproducible elsewhere.

According to guidelines distributed by the Secret Service last August, the types of information solicited for insertion in the computer—broadened at the insistence of the Warren Commission—included items about:

Those who would "physically harm or embarrass" the President or other high Government officials.

Anyone who "insists upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc."

Those who may qualify as "professional gate crashers."

Participants in "anti-American or anti-U.S. Government demonstrations in the United States or overseas."

In an interview, Thomas J. Kelley, assistant director of the Secret Service for protective intelligence, said the computer name insertions already totaled more than 50,000. The Secret Service is extremely careful, he said, both in evaluating the encoded subjects and in checking to determine that those who receive a printout are entitled to it.

But there apparently is no formal guideline or list of criteria for dissemination, as there is for insertion. And direct, automatic, teletype access to the computer from distant Secret Service bureaus—the system used by the airlines and the National Crime Information Center—may be the next step, Mr. Kelley said.

Nothing demonstrates how remote access multiplies the output of a computer better than the crime information center's system, staged by the F.B.I. in 1966.

With direct-access teletype terminals in 21 state capitals and large cities, the information center computer here can be queried directly by local police departments on the names, aliases, Social Security numbers, license tag numbers and a broad array of stolen goods (including boats) that come hourly before the police.

An officer in a patrol car tailing a suspicious car can radio his dispatcher, ask for a check of a license number, and be told by teletype and radio in less than a minute that the automobile is stolen and that its occupants may be "armed and dangerous."

With one of the newest and most sophisticated random access computers in Federal service the Secret Service data center can also perform some wizardry that no other equipment here can master. It can be ordered, for example, to print out a list of all potential trouble makers—"persons of protective interest"—at the site of a forthcoming Presidential visit. The random access scanning can be geographical.

Photographs and descriptions can be assembled for the traveling White House detail. Investigations, even detentions, can be arranged at the site.

"You take a waiter in a hotel dining room where the boss is going to speak," a Secret Service spokesman explained. "Let's say the computer turns up his name and we investigate and decide it would be better for him to be assigned to some other duties. No one has a constitutional right to wait on the President, you know. That's how it works."

Cued by another more elegant electronic program, the same computer can also produce all the information it contains on the "characteristics" of subjects encoded on its tapes—all the short, fat, long-haired, young white campus activists in Knoxville, Tenn., for example. Only the Secret Service computer can do that.

The American Civil Liberties Union office here protested last October that the Constitution protects such acts as an effort merely to "embarrass" a Government official, the persistence of citizens in seeking redress even of "imaginary" grievances, and their participation in "anti-U.S. Government demonstrations." The Secret Service, however, has declined to withdrew or amend its intelligence reporting guidelines.

"They seem satisfactory to us," Mr. Kelley said. "If we weren't getting the information we want, we'd change them."

Under the heading, "Protective Information," the guidelines read as follows:

"A. Information pertaining to a threat, plan or attempt by an individual, a group, or an organization to physically harm or embarrass the persons protected by the U.S. Secret Service, or any other high U.S. Government official at home or abroad.

"B. Information pertaining to individuals, groups, or organizations who have plotted, attempted, or carried out assassinations of senior officials of domestic or foreign governments.

"C. Information concerning the use of bodily harm or assassination as a political weapon. This should include training and techniques used to carry out the act.

"D. Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.

"E. Information on any person who makes oral or written statements about high Government officials in the following categories: (1) threatening statesments; (2) irrational statements, and (3) abusive statements.

"F. Information on professional gate crashers.

"G. Information pertaining to 'terrorist' bombings.

"H. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war.

"I. Information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas.

"J. Information regarding civil disturbances."

Senator Ervin, who is noted for a piquant sense of humor, said in a speech a few months ago: "Although I am not a 'professional gate crasher,' I am a 'malcontent' on many issues.

"I have written the President and other high officials complaining of grievances that some many consider 'imaginary.' And on occasion I may also have 'embassaised' high Government officials."

Based on the guidelines, the Senator asserted, he himself is qualified for the computer.

[From the Greensboro (N.C.) Daily News, July 1, 1970]

PERSONS OF INTEREST

Are you a "person of interest" to the United States government? You may be whether you know it or not, and regardless of whether you have a criminal record or even an arrest record.

You are if you:

Are a "professional" gate crasher.

Have attempted or plan to attempt, either individually or as a member of a group or organization, to "physically harm or *embarass* the persons protected by the U.S. Secret Service, or any other high U.S. government official at home or abroad."

Have made any oral or written statements about high government officials that might be interpreted as "threatening," "irrational," or "abusive."

Occasionally or regularly "insist upon personally contacting high government officials for the purpose of redress of imaginary grievances etc."

These are some of the guidelines certain federal agencies are using as they quietly build up information (some of it almost certainly false information based on rumors) dossiers on hundreds of thousands of law-abiding, but for one reason or another suspect, American citizens.

Among the federal agencies engaged in this sort of information gathering are the Secret Service, The Federal Bureau of Investigation, Justice Department, Internal Revenue Service and the Army's Counterintelligence Analysis Division. These agencies swap information freely and make their files available to certain other federal agencies.

The agencies involved cite as the source of their authority the recommendations of the Warren Commission. The commission recommended the broadest possible surveillance of "malcontents" and potential assassins. Although the commission's recommendations have not been enacted into law, the federal agencies now in the surveillance business are going far beyond them. Participation in an anti-war demonstration is enough to get on the list.

This is taking place apparently with the tacit consent of a majority of American citizens, possibly because most of them are unaware of the extent of the information gathering and its implications.

The broad language of the guidelines the agencies use is dangerous in itself. So is the practice of integrating the files on criminals with the files on law-abiding citizens. Together with certain provisions of the Nixon administration's omnibus crime bill, such as the preventive detention and "no-knock" search clauses, they lay the ground work for a police state of a sort Americans have never known except by hearsay.

Few public critics of this developing surveillance system have emerged. The only two in Congress are Senator Sam J. Ervin Jr. of North Carolina and Rep. Cornelius Gallagher of New Jersey. Mr Ervin charges that the system is a threat to the right of privacy and a potential infringement of the First Amendment rights of free speech and assembly.

Senator Ervin, chairman of the Senate Subcommittee on Constitutional Rights, takes the view that the government's information gathering about the lives and habits of its citizens is pushing the country toward a mass surveillance system unprecedented in American history." The federal gumshoes are getting by with it because Americans fail to understand the computer mystique and its implications, Mr. Ervin says.

Briefly, the computer mystique is the doctrine that the computer is foolproof, 100 per cent objective, and naturally superior to the human brain that created it. Emotion clearly does not enter into a computer's decisions. And a computer can perform a routine task much faster than a man. But thousands of Americans on computer billing lists know the computer can make the same errors that men make.

The difference is that when a computer makes a mistake it is almost impossible to get it to correct itself without the intervention of the humans who guide it. But it is not in the self-interest of those who program and operate the computer to catch it in too many mistakes. That would tend to undermine the computer mystique upon which their jobs and power depend.

Senator Ervin contends, and we agree, that within the government data files there exists "a potential for control and intimidation that is alien to our form of government and foreign to a society of free men." Based on the guidelines, the Senator told reporters, he is himself qualified for the computer files.

"I have written the President and other high officials complaining of grievances that some may consider 'imaginary.' And on occasion may also have 'embarrassed high government officials," he said.

How do you break up the snoopers' playhouse in Foggy Bottom? The quickest way is to let your congressman and senators know you don't like it. Congress can put the national data bank out of business. Congress will put it out of business when the public demands it, but not before.

[From the Asheville (N.C.) Times, June 18 1970]

BIG BROTHER WINS ANOTHER ONE

Overruling a lower court, the New Jersey Supreme Court has decreed that police agencies in that state may indeed compile exhaustive dossiers on persons who take part in demonstrations—whether or not the demonstrations involved disorder and whether or not the person investigated committed any illegal act.

The range of this Big Brotherism is dangerously wide. It permits the compiling of information on the individual's family, employment, finances, personal habits and past activities. The danger is that it makes people who may have been only inoocent bystanders subject to the most intensive kind of official prying. The mere gathering of the information, which involves police questioning of friends, employers and others, can all too often arouse unjustified suspicion among acquaintances.

This prying trend is by no means confined to New Jersey. It has been revealed recently that Army Intelligence has dossiers on millions of Americans with the only excuse that such persons *might* some day be investigated for sensitive posts in the military establishment. Just recently the White House instigated a check into the personal backgrounds of 250 State Department employees who protested the Cambodian invasion. The FBI of course has voluminous files.

It would seem that the point is right here at which to draw the line on this ever-increasing snooping into the private lives of presently uninvolved citizens. The line should be at the point where an individual has actually applied for a sensitive position, or has actually been involved in illegal disorders. Mere participation in an orderly demonstration should be no authorization to open a file.

North Carolina's Senator Sam J. Ervin has been the leader in Congress in defending federal employees from the often outrageous lengths to which security checks go. He could well lift his sights and take in the whole range of official prying into private lives.

Enforcement agencies have the right and duty to learn all they can about individuals who seek sensitive posts or who are suspected of committing illegal acts. Investigation before the act is indefensible.

Hopefully, the New Jersey ruling will be taken into the federal courts and there overturned. Big Brother has too much power already.

[From the Omaha World-Herald, Jan. 15, 1970]

ERVIN ON GUARD

The trouble with letting government agencies have all those data processing machines is that it helps create a demand for more data to be processed.

This can lead to the government's having much more information than it needs or than is good for it or the country, especially when the information consists of files on individual citizens.

Sen. Sam. J. Ervin, D-N.C., chairman of a subcommittee on constitutional rights, thinks he detects an instance in which the government is trying to collect too much about too many people, and for insufficient reason.

Ervin has questioned the Secret Service's attempt to enlist other government agencies in the compiling of computer dossiers on persons who make threatening, irrational or abusive statements about high government officials; professional gate crashers; persons who insist on personally contacting high government officials for the purpose of redress of grievances, or people who take part in demonstrations.

This sort of information gathering Ervin characterized as "conducive to a mass surveillance unprecedented in American history." He wrote a concerned letter about it to Treasury Secretary David M. Kennedy, whose department includes the Secret Service.

Kennedy replied that the Secret Service limited such activities to its mission of protecting the President and others for whose safety it is responsible.

He said the information Ervin referred to was being sought only from law enforcement agencies, not from "run of the mill" government workers. He also said that the information relating to people who had taken part in demonstrations was required only in connection with the safety of the President while traveling.

Ervin also questioned whether the information the Secret Service was gathering would be in safe hands. He said he was con-

cerned over who would have access to the files.

Kennedy replied that all computer personnel have top secret clearances and that no other persons or agencies had direct access to the files.

That, perhaps, is the key to maintaining continued freedom from mass surveillance by the government. If the information on individuals obtained by one branch or department is kept in its own files and used only for its own necessary purposes, the likelihood of untoward government surveillance is reduced.

However, if all the agencies of government started comparing notes and collecting individual files into master dossiers, Washington could end up with a frightening array of weapons that could be used, at the whim of a bureaucrat, for any number of unsanctified purposes.

Sen. Ervin has suggested several approaches to computer control and legislative safeguards, including prohibitions on transfer or use of data collected for one purpose only.

Perhaps, in the case of the Secret Service, nothing particularly ominous is involved in the gathering of information. At least Secretary Kennedy's reassurances to Sen. Ervin sound convincing.

But this assuredly will not be the last time when the government's use of information gathering and storing techniques will be called into question. The best way to keep 1984 from getting here before it is due on the calendar is to be alert to the dangers, and we hope Sen. Ervin and others will continue to be.

[From the Sioux Falls (S. Dak.) Argus Leader, Jan. 16, 1970]

A HINT OF BIG BROTHER

Sen. Sam J. Ervin of North Carolina, chairman of a Senate subcommittee on constitutional rights, has expressed concern about what he sees as a new threat to First Amendment freedoms.

The threat, he fears, is embodied in new Secret Service guidelines for gathering and storing information about many citizens. Ervin has performed a valuable public service by calling attention to this matter.

It is the old story: Little exception could be taken to what the Secret Service is doing if there were firm guarantees against misuse of the data, but there are no guarantees.

Congress had better get busy and provide for some. Ervin thinks "the criteria for filing information about individuals are questionable from a due process standpoint, are impractical and are conducive to a mass surveillance unprecedented in American history." That is something to worry about.

[From the New York Post, June 30, 1970]

BIG BROTHER'S NEW TOYS

There has been little response on Capitol Hill to disclosures about the government's growing industry in recording the names and activities of "malcontents" on its computerized and microfilmed tapes. But the Senate's leading lecturer on Constitutional law, Sam Ervin (D-N.C.), has suggested that under the government's criteria, he could well be suspect.

According to Secret Service guidelines, among the dissidents the computer should know about are:

—Those who would "physically harm or embarrass" the President or other high officials.

—Those who seek personal contact with high officials "for the purpose of redress of imaginary grievances."

Obviously there's room there for more than just one Senator.

Consider the phrase "imaginary grievance." To whom is a grievance imaginary—the lawmaker who brings it or the official who rejects it? The answer, of course, is the official; he's also the guy with the computer.

That section, then, nets all of Sen. Ervin's colleagues in Congress. The only remaining Capitol Hill figure unaccounted for is the president of the Senate, Vice President Agnew, and he could fit the composite for section one.

That he feels to embarrass the President has been adequately proven. That he might physically harm him would seem implausible. But it should be noted that he has had to look elsewhere than the White House for his golfing companions and tennis partners.

[From the Washington Post, Apr. 24, 1970]

IN THE NAME OF SECURITY

A fear of unorthodoxy is the first symptom of insecurity. It marks national administrations that have no clear sense of purpose or direction. Such administrations quite naturally, like a stream seeking its own level, tend to seek in their personnel mediocrity, conformity, conventionality. Innovation frightens them; dissent dismays them. And so they bar from employment anyone who has ever displayed any signs of eccentricity or independence. It is all the more disquieting that such a system of selection is always undertaken in the name of national security. It operates, manifestly, to diminish security rather than enhance it.

Sen. Sam J. Ervin Jr., chairman of the Senate's Constitutional Rights Subcommittee wrote to the chairman of the U.S. Civil Service Commission last week to inquire about report "new rules governing qualifications for federal employment which would exclude persons who have engaged in demonstrations and protests." The CSC says that no new rules have been adopted; the old rules are simply being applied with a bit more stringency. In this connection it is alarming indeed—although by no means surprising—to learn that the Civil Service Commission maintains a blacklist containing the names of at least 1.5 million Americans who might, at some time, have been involved in "subversive activity." The blacklist is largely compiled, without any fixed standards, from references to individuals in the publications of so-called radical student movements.

Shades of Titus Oates and Joe McCarthy! These scraps of information squirreled away in the files of the CSC are like so many pellets of deadly poison. Although they are not supposed to be taken in themselves as proof of subversive activity or intent, they operate inevitably, nonetheless, as flags disqualifying their subjects for federal employment. The injustice of this system to the individuals damaged by it is the least of the problem. The worst of it is the impact on the public service. As Senator Ervin observed, it is essential to assure that any denial of a security clearance or of a federal job is rendered on equitable, just and timely standards of social behavior. Otherwise we face dangerous conformity in our national life and a bleak future of mediocrity in the federal service.

[From the Asheville (N.C.) Citizen, July 2, 1970]

YOU CAN BE A PERSON OF INTEREST

Despite the fact that a few voices are raised in opposition—notably that of Senator Sam J. Ervin—intelligence agencies of the Federal government are still quietly compiling informational files on hundreds of thousands of law-abiding—though presumably suspect—Americans.

Declaring that violent political dissent and civil disorder require the policy, the government is building a mass of computerized information on "persons of interest."

The phrase is a term for those citizens, many with no criminal records, whom the government wants to keep track of, just in case trouble breaks out.

The files often contain seemingly unimportant data, which can be shared—almost instantaneously—by half-a-dozen intelligence gathering groups.

The operation does not disturb us particularly, though it is unauthorized by law and raises serious constitutional questions.

Critics claim the computerized "who's who" is leading the country toward a police state.

Possibly so, and much of the action seems senseless. But think what a convenient tool the files would be if the country—God forbid—ever drifts toward dictatorship.

[From the New York Times, July 4, 1970]

OUR ALIENATED RIGHTS

One hundred and ninety-four years ago the Founding Fathers asserted their independence with a ringing Declaration of man's "unalienable rights."

Today, as too often before, those rights are once more threatened. They are threatened not by some tyrannical foreign monarch, but by domestic governmental agencies whose actions and proposed actions against crime and dissent endanger constitutional guarantees designed to safeguard the rights of Americans to "life, liberty and the pursuit of happiness."

Typical of these new dangers is the spreading web of Federal prying into the private lives of citizens. Utilizing modern computer technology, Federal police, security, military intelligence and other agencies are accumulating vast stores of data on the activities of hundreds of thousands of unsuspecting "suspect" Americans.

There is nothing wrong with the use of the computer to help make more efficient and effective the legitimate work of law-enforcement and other agencies. A modern society must use modern techniques to help enforce and administer its laws and to protect itself from those who would do violence to its leaders and institutions.

But a subcommittee headed by the highly respected Senator Sam J. Ervin Jr., Democrat of North Carolina, has unearthed alarming evidence that Federal agencies have been employing the new technology to amass data that has little or no direct relation to criminal or other activities of legitimate Federal concern. Particularly disturbing are persistent reports that the Army's Counterintelligence Analysis Division is disregarding orders to stop collecting information on peace and civil rights organizations. Furthermore, the subcommittee reports that restrictions on the dissemination of "intelligence" accumulated by some agencies is woefully inadequate.

Among the "persons of interest" on whom the Secret Service collects data are individuals who have merely threatened to "embarrass" a high Government official, who "insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.," and who participate in anti-American or anti-United States Government demonstrations.

Senator Ervin, a conservative and a student of the Constitution, has observed: "I am a 'malcontent' on many issues. I have written the President and other high officials complaining of grievances that some may consider 'imaginary' and on occasion I may also have 'embarrassed' high Government officials."

Senator Ervin is obviously a "person of interest" by Secret Service definition and therefore grist for a Federal computer. Indeed, any American today who vociferously articulates unpopular or unorthodox views is in danger of being digested by a Federal computer, along with common criminals, and of being exposed to potential harassment and humiliation.

If Americans still cherish the Declaration of Independence and the rights we celebrate

today, they will insist that their representatives in Congress support Senator Ervin's efforts to place strict legal limits on Federal collection and dissemination of information on the activities of private citizens.

[From Computerworld, Aug. 27, 1969]

PRIVACY LOST?

The bill to implement President Nixon's national computerized job bank program does give the secretary of labor the power to prescribe "rules and regulations to assure the confidentiality of information submitted in confidence" to one of the banks.

But nowhere is there any mention of the key point made by President Nixon during his election campaign. At that time, he stressed that only jobs would be stored. Applicants would not have to insert their names, he said, only their qualifications. This would assure privacy and eliminate any possibility that additional personal records would be gathered and stored.

While the absence of this precaution from the bill does not mean this safeguard will not be included in the final program, we would be much happier if it were spelled out in the bill.

POLITICAL PRESSURE NEEDED

At present, the individual has no protection against the use or misuse of personal information in data banks, and it now appears that it will be several years before adequate protective legislation can be formulated.

But the most important data banks are being set up now, and there is a need for immediate protection. Several congressmen have suggested that a person or group be named as a data bank ombudsman, with the power and responsibility to protect the individual against the misuse of information in data banks.

Such an ombudsman provides an immediate solution to an immediate problem. And he would also help to find a long-term solution, because he would be able to use his experience to help formulate laws regulating data banks.

Ombudsmen should be appointed on both the state and federal level. But the appointment of such ombudsmen will occur only if pressure is brought on legislators now. This is an election year and consumer protection is an important issue—congressmen and state legislators will be more responsive this year than at any other time.

We propose that individuals and local chapters of professional societies immediately begin a campaign for data bank ombudsmen. Such a campaign should be primarily educational at first: informing local newspapers, state legislators, and congressmen of the dangers posed by computerized data banks and proposing the appointment of ombudsmen as an immediate solution. And we must keep the pressure on.

Data bank ombudsmen offer the only hope of protecting the rights of the individual in the near future. Concerted action by computer professionals could make such protection a reality.

[From the Washington Evening Star, Mar. 16, 1970]

PRIVACY AND THE COMPUTER

The cliche about people having skeletons in their closets is woefully out of date. These days, the skeletons are in computerized data banks. What's worse, the figurative skeletons may be mislabeled with the wrong owners' names, or they may be the figment of a computer's imagination.

The dangers of the mysterious, hard-to-refute data banks have been much discussed in the last few years. The discussion is about to accelerate again, and it's a good thing, because eventually something may be done about the problem.

The National Academy of Sciences has a $149,500 Russell Sage Foundation grant to conduct a broad study of how to preserve privacy and civil liberties against the onslaught of the computer age. The study will be conducted by Columbia Professor Alan Westin, an expert on the subject, and will focus on how to protect the rights of persons (meaning everybody) on whom information is collected and stored for a variety of uses. Westin will be backed by a panel including Ralph Nader, James Farmer, former Attorney General Katzenbach and Representative Cornelius Gallagher of New York, who heads the House subcommittee on invasion of privacy.

On another front, House committee hearings are to start tomorrow on the proposed Fair Credit Reporting Act, which already has Senate approval. The bill aims at giving consumers a way to counter erroneous or malicious information on file against them in credit data banks. Included in the bill's provisions are rules to limit disclosure of information, to let the consumer know what's in his own file and to give him the right to dispute the information.

Still dormant is the 5-year-old proposal for a National Data Bank, a menacing centralization of the information collected by federal agencies. The plan raised congressional howls in 1966 and was quickly put down as an Orwellian step toward Big Brotherism. But don't count it out—it makes too much computer-type sense to have one big control panel able to spill the beans on all our lives.

Future studies are likely to add to the growing pile of horror stories about people whose lives were marred because a computer dredged up some embarrassing fact from the sooner-forgotten past—or from nowhere. It's too bad the comprehensive National Academy of Science investigation, which could lead to important reforms, is scheduled to take 2½ years. Because that will bring us 2½ years closer to 1984.

[From the Houston (Tex.) Post, Mar. 16, 1970]

DATA BANK IDEA ALIVE

The proposal advanced a few years ago to establish a national "data bank" in which information collected by federal agencies would be stored and made available at the push of a computer button appears to be far from dead.

It is being talked up again, at least sufficiently for Sen. Sam J. Ervin of North Carolina, chairman of the Senate's subcommittee on constitutional rights, to say that he will reopen the hearings this year.

Despite assurances that there would be all kinds of safeguards to protect the privacy of individual citizens, the mere thought of the pooling of all the information gathered by government agencies was enough to arouse in the minds of a great many people Orwellian nightmares of a "Big Brother" watching their every move constantly.

Even though it was promised that the stored information would be impersonal and not linked with any individual, being of the general type collected by the Census Bureau, there were fears that once the information bank should be established, this could be changed. It would be a relatively simple matter to compile and file away a fairly complete dossier on every citizen, containing all kinds of highly personal information. This information might or might not be accurate.

The great fear was that any concentration of data could be abused and the information misused, perhaps not immediately but at some time in the future. The instinctive reaction of most people that it would be much safer, so far as the privacy and perhaps the freedom of the individual citizen is concerned, not to permit the proposed "bank" to be created.

Potentially, there could be a great concentration of power in the hands of whoever assembled and controlled the information, and it is elementary that the diffusion of power is the best protection against tyrannical government.

Federal agencies now collect a great deal of information about a great many people in the course of their normal operations, but the data collected by one in most cases is not available to the others. For the "data bank" idea to be acceptable to most people, it would be necessary that there be strong restrictions upon the information that is pooled, on how it is to be used and to whom it is to be made available. It remains for advocates of the idea to prove that adequate, foolproof safeguards against misuse and abuse are possible.

Although efforts to establish a national "data bank" have been blocked thus far, vast quantities of highly personal information already are stored in computers about practically every American citizen, and if the data ever should be brought together, it would make fairly complete dossier on him and all of his personal affairs.

The tremendous expansion of this country's credit system has made necessary the compilation of information about everybody who buys anything on credit. It is necessary for those who extend credit to know a great many facts, much of it very personal, about those seeking credit to determine how good credit risks they are. This has given rise to many private agencies that collect this information. Many of these co-operate and exchange information.

It is estimated that one credit agency alone has data on millions of Americans on file in its computers. Every time a citizen draws a paycheck or answers a census question, the information is recorded on somebody's computer somewhere.

There is relatively little reason for alarm in this because the information is fragmentary and widely scattered. What arouses concern are continuing efforts to bring all these bits and pieces of information together in one vast computer bank, with the possibility that the data might fall into the wrong hands and/or be misused.

[From the New York Times, July 7, 1970]

IN THE NATION: A RIGHT NOT TO BE DATA-BANKED?

(By Tom Wicker)

WASHINGTON.—Do you have a right not to be stored in a computer, where you can be called up for instant investigation by any bureaucrat or law officer who considers you a "person of interest" or who may want to provide someone else—maybe your employer—with "facts" about you? If you haven't thought about that, it's high time you did.

Ben A. Franklin detailed in The New York Times of June 28, for example, how Government "data banks" are mushrooming out of computer wizardry. Literally hundreds of thousands of individual dossiers now are being stored on tape by various agencies. The tape can be fed to computers with instant recall; and the computers and tapes can be interconnected from one agency or region to another in an ominous national network. Numerous state agencies have easy access to the material in this computer network, and are under little or no pressure to keep it confidential.

At the very least, therefore, some guidelines on the compilation of these banks and some safeguards on disseminating the material appear in order. An interesting case pending in Federal court here (*Menard* v. *Mitchell* and *Hoover*) may help provide them.

A Maryland man was arrested in California in 1965 on suspicion of burglary, held for two days, then released when police found no basis for charging him with a

crime. Subsequently, a brief record of the detention, together with the Maryland man's fingerprints, appeared in F.B.I. criminal files.

Maintaining that the record is misleading and incomplete and that it is not properly a "criminal record," the Maryland man moved in Federal District Court here to have it purged from the F.B.I. files.

COURT CONCERN INDICATED

The Court denied this motion, and the man appealed. On June 19, the Court of Appeals for the District of Columbia, while finding no fault with the district court's ruling on the motion, ordered the case remanded for trial and "more complete factual development. The supporting opinion, although limited to the case, suggests the circuit court's concern about what ought to go into Government files, under what rules, and whether proper safeguards surround its dissemination.

The judges (Bazelon, McGowan and Robinson) pointed out that the fact that the police had been "unable to connect" the Maryland man with a crime did not necessarily acquit him of having committed one, and they conceded that certain arrests not followed by a charge or a conviction might be a proper part of someone's criminal record. But, they asked, did the mere fact that a man had been picked up and held for two days justify the F.B.I. in retaining the record in its criminal identification files?

An arrest record (the distinction between a "detention" and an "arrest is considerably less than a difference) can be terribly damaging to one's opportunities for schooling, employment, advancement, professional licensing; it may lead to subsequent arrests on suspicion, damage the credibility of witnesses and defendants, or be used by judges in determining how severely to sentence. Moreover, thousands of arrests are made every year without any further action against the arrested person, usually for lack of evidence.

DISSEMINATION ISSUE

Thus, the court asked, if a person is arrested, even properly, but no probable cause for charging him is developed, should he "but subject to continuing punishment by adverse use of his 'criminal' record?"

This has particular point because of the lack of established safeguards on dissemination. The Maryland man's record, for instance, could be made available by statutory authority to "authorized officials of the Federal Government, the states, cities, and penal and other institutions" and also, by an Attorney General's regulation, to government agencies in general, most banks, insurance companies, and railroad police.

When New York recently passed a law requiring employes of securities firms to be fingerprinted, several hundred were dismissed for "criminal records," but about half of them had only arrests, not convictions, on their records. The Appeals Court, noting this, reasoned that F.B.I. records had been passed directly to the securities firms involved.

As data banks proliferate, so will the indiscriminate use of the material they contain. And that raises the question whether an American citizen has a constitutional or legal right not to be data-banked, computerized, stored exchanged and possibly damaged—materially or in reputation—by the process.

[From the Huntsville (Ala.) Times, July 12, 1970]

"MAFIA MACHINE" GOES TO WORK

(By Jared Stout)

WASHINGTON.—A computer nicknamed the Mafia Machine has gone to work in the Justice Department, giving organized crime fighters their most powerful weapon to date. But it may be a mixed blessing.

While the machine is enabling heretofore impossible analysis of the activities of organized criminals, it is also raising new questions about computers in law enforcement and invasion of individual privacy.

Within the computer's memory, the department is storing histories of the major and minor figures in confederated crime, how and where they travel, even details on their eating habits.

But the department is also computerizing the names of those legitimate individuals with whom the Mafiosi often deal, persons against whom no charges have been brought or proved.

Thus while members of the Organized Crime and Racketeering section are highly pleased with the workings of their still embryonic system, they are deeply troubled by the privacy issue.

"I feel like I'm walking around with a bomb in my hands," said one official who has worked on the project and who declined to be quoted by name. "Some of this information is really dynamite."

"The fact is the privacy issue is one of paramount importance and we haven't yet figured out a way to balance the law enforcement needs with the constitutional safeguards for privacy," the official said.

For the moment, however, the privacy question is being put to one side as the department fine-tunes the computer and explores its use in analysis of what's going on within the organized crime community.

Individuals now included within its memory against whom there may be no more than a suspicion—a person who, for example, is frequently seen in the company of a known hoodlum—are protected by tight security.

According to the department, only law enforcement, agencies with a need to know are given information drawn from the computer, and they insist that individuals listed because of unverified suspicions are made known to none outside the federal investigative family.

The basic data for the computer has come from reports given the organized crime section by 26 other federal agencies, principally the FBI, the Internal Revenue Service and others that regularly join the section in cooperative investigations.

The information is, however, keyed into portions of the 400,000 file cards containing 250,000 names of Mafia or Mafia-related individuals.

Until six weeks ago, the file cards were the major source of section information, a system that prevented recall of the data they contained without spending days, perhaps weeks, of manual sorting.

The computer makes possible high-speed searches of the records the section has incorporated within its memory, yielding up in minutes, for example, a list of all those Mafia figures nicknamed "Sonny."

Such information becomes useful because the operators of big crime often speak of one another only in nickname references.

Gerald Shur, the man-in-charge of the computer program, said in a recent interview "the kinds of questions we can ask are limited only by the data we can feed into the computer."

Shur said ultimately the department hopes to store enough information to enable predictions about the impact of investigatione or develop economic theories to estimate what kinds of business situations organized crime may be heading toward.

[From the Boston Herald Traveler]

BIG BROTHER (U.S.) IS WATCHING YOU

(By John S. Lang)

(NOTE.—The government knows far more about you than you may euspect. And if you've ever taken part in protest marches or the like, even the military services probably have been keeping tabs on you. Some agents have seized garbage in hunting incriminating evidence.)

WASHINGTON.—Behind the closed door of Room 2439, a handful of government clerks search through radical newspapers, methodically snipping out names. They are hunting Americans favorably mentioned by the publications of dissent.

Found, snipped, checked, reviewed, the names are conveyed down a wide clean corridor to be fed into a "subversive activities" data bank already bulging with names of 1.5 million citizens.

The name-hunters in Room 2439 are low-level servants of the Civil Service Commission, the agency set up to oversee federal employment.

The commission's security dossier—not to be confused with its separate files on the 10 million persons who have sought federal jobs since 1939—are indicative of the watch the government keeps on Americans in this age of dissent and social turmoil.

An Associated Press study showed:

Military intelligence agents have spied on civilian political activities and kept secret computerized files on thousands of individuals and organizations although Pentagon counsel cannot cite any law authorizing this surveillance.

The Army has kept a so-called blacklist which included the names, descriptions and pictures of civilians "who might be involved in civil disturbance situations."

A second list has been circulated by the Pentagon's counter-Intelligence Analysis Division as a two-volume, yellow covered, loose-leaf publication entitled "Organizations and Cities of Interest and Individuals of Interest"—according to a court suit.

The FBI, with the most extensive security files and 194 million sets of fingerprints, has infiltrated the leadership of virtually every radical organization in the United States.

Agents of the FBI, Naval Intelligence and local police have seized citizens' garbage in hunts for incriminating evidence. In one case Navy agents examined garbage from an entire apartment house to find information about one tenant.

The Secret Service has set up a computer with 100,000 names and 50,000 investigative dossiers on persons who it says could be dangerous to top government officials.

A Senate subcommittee found that federal investigators have access to 264 million police records, 323 million medical histories and 279 million psychiatric dossiers. In each category, that's more numbers than there are people in the United States.

And the massive files of investigative and intelligence agencies contain but a small portion of the information the government collects on its citizens.

Millions of scraps of information go into federal files routinely when citizens pay their taxes, answer the census, contribute for Social Security, serve in the military, or apply for a passport.

In fact, a Senate subcommittee calculated that the names of U.S. citizens appear 2.8 billion times in federal records. This means, the panel said, that the statistical odds are that a dozen different agencies have files on the typical law-abiding citizen.

Much of this data is held in strictest confidence. Census questionnaires, for example, can be inspected only by Census Bureau employes—and they're sworn to secrecy.

Federal income tax returns also are considered confidential by the IRS. But they may be seen by the heads of federal agencies, some congressional committees, the governors of every state and by a special counsel to President Nixon.

A proposal three years ago to gather files of all agencies into a National Data Bank and use them for statistical purposes kicked up such a furor in Congress that, according

to one official, "now that issue is dead as a dodo."

But the AP study showed that investigative and intelligence agencies can—and do—share the information they gather.

For example, investigative agencies of the executive branch have access to the "subversive activities" data bank in the Civil Service Commission's downtown Washington headquarters.

According to an official commission publication, the data bank "at present . . . contains approximately 2.5 million index cards containing information relating to Communist and other subversive activities."

The document adds: "No information is added to this file until it has been determined after careful review by a responsible official who is experienced in this field that an actual question of subversive activity is involved. . ."

A quick thumbing through the file discloses names like:

Charles Garry a white San Francisco attorney who represents the Black Panthers.

Robert Shelton, a leader of the Ku Klux Klan.

Staughton Lynd, a professor and radical writer.

Robert DePugh, head of the Minutemen.

The files are kept as index cards in mechanized rotary cabinets. There are thick bundles of cards for some individuals, only one card for others. The cards do not state anything about a person; they are more like a bibliography, citing publications which mention him. Until evaluated, the clippings are considered "raw data" and are kept in other filing cabinets.

One name in the raw data is that of William Kunstler, civil rights attorney who represented the defendants in the "Chicago 7" conspiracy trial and who faces a jail term for contempt of court.

Kimball Johnson, director of the commission's Bureau of Personnel Investigations, says the security file is kept up to date by 17 clerks, "experts in the field," who read Communist publications, the Black Panther newspaper, the free presses, underground papers and other publications such as The Guardian, Workers World, The Militant and Liberation News Service.

"We read these and clip the names of people supported by them," Johnson says. "It's all in the public domain. It's simply that unless you clip it and title it there's no one mind that can comprehend it."

Section Chief Pierce waves a hand toward a stack of publications on a table in his office and says: "That's what we check. It's full of subversive material. Note the Commie art, Picasso and others all tied in to Communism."

Asked to cite a statute or regulation authorizing the security file, Johnson replied there is no specific law. But, he added:

"The file is an essential tool to the commission's legal function of investigating the fitness of people for federal employment for security positions. And there is Public Law 298 which shifted responsibility for making personnel investigations from the FBI to the Civil Service Commission."

The commission says its security file aids in personnel investigation which give "the reasonable assurance that all persons privileged to be employed in . . . government are reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States."

It also says that when any subversive information from the security file is identified with a person under investigation the case is referred to the FBI for a full field loyalty probe.

The FBI has overall responsibility and broad powers—based on presidential directives dating back to 1939—for investigating matters relating to espionage, sabotage and violations of neutrality laws.

FBI Director J. Edgar Hoover told Congress last year his agency had placed informants and sources "at all levels including the top echelon" of such groups as the Student Nonviolent Coordinating Committee, the Ku Klux Klan, the Black Panther Party, the Republic of New Africa, the Nation of Islam, the Revolutionary Action Movement, the Minutemen and the Third National Conference on Black Power.

Hoover also gave a hint of the scope of FBI security files when he outlined how agents keep tabs on sympathizers *who contribute money for radical causes.*

"Included among these," he testified, "are a Cleveland industrialist who has long been a Soviet apologist, the wife of an attorney in Chicago who is a millionaire, an heiress in the New England area who is married to an individual prominent in the academic community who has been active in New Left activities, and a wealthy New York lecturer and writer who for years had been linked to more than a score of Communist-front organizations and has contributed liberally to many of them.

"These individuals alone have contributed more than $100,000 in support of New Left activities."

Hoover also said agents have identified most of the writers of antiwar newspapers—which he termed "the work of the dedicated revolutionaries who are against ROTC and against our war effort in Vietnam"—and had referred that information to the Justice Department for possible prosecution.

Don Edwards, a member of the subcommittee which oversees FBI budget requests, complains that Congress does not exert proper authority over the FBI. He believes one reason for this is fear stemming from long standing rumors that the FBI, among its many dossiers, has files on each member of Congress.

"There are lots of congressmen who think that probably they do have files," Edwards told an interviewer.

But the rumors have never been proven and there have been few complaints from congressmen.

There was, however, much alarm expressed in Congress with the recent disclosure that, for the past several years, military intelligence agents have conducted surveillance of civilian political activists and have fed information on individuals and organizations into data books.

In response to 50 congressional inquiries, the Army admitted that it:

Kept a so-called blacklist which included the names and descriptions and pictures of civilians "who might be involved in civil disturbance situations."

Operated a computer data bank for storage and retrieval of civil disturbance information.

Used its intelligence agents in some instances for direct observation and infiltration of civilian organizations and political meetings.

But in making these admissions, the Army said that during the past year it has sharply curtailed such activities after realizing they weren't needed to prepare for any civil disturbances.

The Army said the blacklist—a term to which it objected—had been ordered withdrawn and destroyed. It said the computer data bank had been discontinued and that its agents have conducted no overt operations in the civilian area during the past year.

Extensive details of the military's domestic intelligence activities were disclosed in January in an article written by a former intelligence officer, Christopher H. Pyle of New York, for the Magazine Washington Monthly.

Pyle wrote that the Army's Intelligence Command, headquartered at Ft. Holabird, Md., was in a position to develop one of the largest domestic intelligence operations outside the Communist world.

A few weeks later, the Pentagon announced that Ft. Holabird would be closed in an economy move and the Army Intelligence School there would be moved to Arizona.

An Army spokesman said the domestic surveillance operations were expanded in 1967 after the outbreak of serious civil disorders.

"There was a feeling we had to be in a position to predict when federal troops would be used again. We need more information to inform tactical commanders on the streets and to guide them. This led to widespread collection efforts," he said.

The information gathered by the military was funneled into Ft. Holabird, summarized and sent out on the Army's Teletype system.

One weekly summary, marked "Pass to DIA Elements," was distributed to Army commands throughout the world. It contained this dispatch:

"The Philadelphia chapter of the Women's Strike for Peace sponsored an anti-draft meeting at the First Unitarian Church which attracted an audience of about 300 persons. Conrad Lynn, an author of draft evasion literature, replaced Yale chaplain William Sloan Coffin as the principal speaker at the meeting."

Lynn, the Women's Strike for Peace and a dozen other individuals and groups identified in the summary have filed suit through the American Civil Liberties Union, claiming the Army has violated their constitutional rights of free speech and association.

The suit, filed in U.S. District Court in Washington, contends that in addition to the surveillance and computer operations the Army admits conducting, it is concealing from Congress the existence of:

A large microfilm data bank on civilian political activity indexed by computer and maintained by the Counterintelligence Analysis Division.

A second computerized domestic intelligence data bank maintained by the Continental Army Command at Ft. Monroe, Va., as well as extensive regional files at other locations.

The "two volume, yellow-covered, looseleaf publication entitled Counterintelligence Research Projects Organizations and Cities of Interest and Individuals of Interest, which describes numerous individuals and organizations unassociated with either the Armed Forces or with domestic disturbances."

The Army said it would not comment on the lawsuit's charges.

But, in an interview, a spokesman for the office of the Army's chief counsel could cite no legal basis for surveillance of civilian activities.

"In the civilian sphere the FBI has jurisdiction," the spokesman said. "We must get approval for what we do from the FBI. There is no specific law on domestic intelligence as such applying to the Army."

To determine the range of domestic military surveillance, The Associated Press submitted a list of 20 questions to each branch of the service. Army spokesmen declined to answer the questions specifically, preferring to speak generally about the program. The Air Force said it does not have any domestic program. The Navy never responded.

But Navy intelligence operations slipped into public view last August when the ACLU complained that agents were sifting through garbage from the apartment house of Seaman Roger Lee Priest accused by the Navy of soliciting members of military forces to desert in an underground newspaper he published.

A spokesman for the District of Columbia government acknowledged garbage from all apartments in the building where Priest lived was searched because it couldn't be

separated from the seaman's prior to collection.

"We ended up with an ONI agent posing as a sanitation worker and picking up trash and bagging the garbage," he said.

"Then the Civil Liberties union got in, raising hell."

Searching citizen's garbage apparently is not uncommon for government security agencies. Last summer a D.C. Sanitation Department official disclosed that the city, on request of investigators, makes up to a dozen special garbage collections yearly "in the interests of law and order."

Besides garbage, private mail also is often watched by government law enforcement agents.

The most commonly used means is the "mail cover," recording from a letter the name and address of the sender, the place and date of postmarking and the class of mail.

The Post Office declines to say how many mail covers are in effect. A Senate committee asked for a list of several years ago, but the agency objected.

"The list you have requested would contain the names of about 24,000 persons, a large percentage of whom are innocent of any crimes," a postal official said.

More recently, the Post Office confirmed a new regulation allows federal agents to open all mail coming into this country frim virtually every nation in the world.

"However," a spokesman said, "it's not intended to be used on personal mail."

When thrcatening letters are received by the President or other high government officials, the Secret Service moves into action.

Operating under guidelines adopted after President John F. Kennedy's assassination, the agency collects "protective information" which is fed into its computers.

One of the 1963 guidelines asked other federal agencies to relay information on citizens who make abusive statements or attempt to "harm or embarrass" high government officials.

Civil libertarians objected that this guideline means that any citizen who writes a strongly worded letter of complaint to a government official might come under the agency's scrutiny.

A Secret Service spokesman responded: "At the time the guidelines were passed emotions were high. Everyone was saying, 'Let's protect the President.' Now people are apparently forgetting the tragedy of that year . . ."

Several years ago when Congress was considering proposals to establish a National Data Bank to gather files from all agencies and use them for statistical purposes, author and sociologist Vance Packard raised the spectre of Big Brother, the symbolic totalitarian government in George Orwell's book "1984."

Noting that the year 1984 would come in the next decade, Packard told a congressional committee:

"My own hunch is that Big Brother, if he ever comes to the United States, may turn out to be not a greedy seeker, but rather a relentless bureaucrat obsessed with efficiency."

[From the Morning Call, (Pa.) June 30, 1970]

GUARDIAN OF FREEDOM

Sen. Sam J. Ervin Jr. is a conservative Democrat from North Carolina. But he is also a guardian of constitutionlly guaranteed freedoms.

Sen. Ervin is currently worried about the massive record-keeping which has come into vogue in government agencies. And press reports concerning the type of records being kept give substance to his fears.

It is all very well for the FBI to utilize computers to process information on criminals and persons sought in connection with crimes. This type of service has been credited with speeding the apprehension of suspects.

But it is a different matter when the Justice Department, the government's prosecutor, maintains dossiers on participants in peace rallies and welfare protests. Moreover, Justice takes it upon itself to categorize such persons as "radical" or "moderate" although it is unclear upon what criteria it bases this distinction.

The Secret Service, which says it is trying to spot potential assassins, also has recourse to the computers: It keeps files on miscontents, persistent seekers of redress and those who would "embarrass" the President or other high-ranking government officials.

These are just a few of the agencies which maintain voluminous files on the activities of citizens in a wide variety of fields. The reasoning behind this extensive bookkeeping is valid. Agencies believe that to be forewarned is to be forearmed. In brief, it is a continuing hunt for potential troublemakers.

But when the government gets into the business of gathering intelligence about its own citizens, it can easily go too far. And there is evidence that it has already done so.

For what reason should an agency keep notes on persons who are doing nothing more than exercising their right to freedom of speech, assembly and petition? Since when has it become a crime to persistently seek redress of grievances?

When it gets into these areas, government is dangerously close to trampling on constitutional freedoms and on the individual's right to privacy. It is easy to see how Sen. Ervin reached the conclusion that such methods have "the potential for control and intimidation that is alien to our form of government and foreign to a society of free men."

[From the Advance, July 19, 1970]

MITCHELL DEFENDS JUSTICE DEPT.'S "BIG BROTHER" ROLE

(By Jared Stout)

WASHINGTON.—The Justice Department has asserted a virtually unchecked right—not subject to the Constitution—to keep records on persons who are "violence prone" in their protests of government policies.

The right, Atty. Gen. John N. Mitchell said through a spokesman, arises from the inherent powers of the federal government "to protect the internal security of the nation. We feel that's our job."

It was the first time Mitchell had outlined the legal basis for the collection and computerization of dossiers on protesters within the department's special Civil Disturbance Unit.

The assertion matches in breadth the claim made June 13, 1969 when the government said it had unlimited powers to eavesdrop on those the Justice Department thinks are seeking to "attack and subvert the government by unlawful means."

The eavesdropping claim was made in defense of electronic eavesdropping against some defendants in Chicago Seven riot conspiracy trial.

The extension of this doctrine to the department's domestic intelligence operation came in response to questions arising from Mitchell's news conference last Tuesday.

Mitchell declined to give the legal foundation for the intelligence operation last Tuesday. He said only "there are no court decisions that would restrain us from compiling this type of information."

Later, however, he acknowledged through the department's spokesman that the legal argument used to justify the Chicago Seven eavesdropping also applied to the intelligence operation.

In the Chicago case, the department said nothing in the Constitution's ban on unreasonable searches and seizures limits the powers of the President—and the Attorney General—to eavesdrop, and now keep records on, those who try to "foment violent disorders."

This position has been sharply attacked by critics including Sen. Sam Ervin Jr. (D–N.C.) as a step toward "a police state" and a potential violation of First Amendment rights to free speech and association.

Earlier this past week, it was disclosed that Treasury Department agents had been seeking the names of those who had checked out books on bombs and explosives from public libraries in Atlanta and other cities.

Ervin attacked this step as he has other intelligence efforts, including those of the Secret Service which lists in computer files all those who may pose a threat to the President.

Throughout his opposition to such activities, Ervin has stressed the lack of standards in deciding who shall be listed within such files, and how once a person is catalogued, he may learn of the step and question his inclusion.

The Justice Department spokesman said the definition of "violence prone" persons for its purposes included those who either acted violently, counselled violence or appeared in the ranks of violent confrontations.

He said the dossiers were not kept on "as broad a range as those compiled by the Army," a reference to the watch military intelligence agents have kept on civilian protesters. No notice is given to those whose names have been recorded.

According to the spokesman, this means those individuals listed in department records at least had to be present or in the leadership of violent events. Army records included, for example, those who subscribed to New Left publications.

It was learned, however, that the justice intelligence unit still has access to the records compiled by the Army, which said in February it had discontinued its record-keeping but has hung on to those it made in four years from 1966.

[From the World News, Roanoke, Va., Mar. 11, 1970]

JUSTICE DEPARTMENT KEEPS FILES ON ACTIVISTS

(Note.—In the last few weeks members of Congress have responded with cries of outrage to a magazine article that reported on how the Army was maintaining a computerized data bank on persons it considered politically dangerous. As a result, the Army announced it was closing down the data bank and that it only began it because the Justice Department, which is responsible for political intelligence functions, was unable to handle them. Now the Justice Deparmtent says it is ready to take over. Morton Kondracke, who reported the government's political intelligence activities in this article.)

(By Morton Kondracke)

WASHINGTON.—While the Army has closed down its political computer, the Justice Department maintains an even bigger one in its "war room" containing data on thousands of individuals, including many whose activities are entirely nonviolent.

Political computers were part of the federal government's response to the problem of controlling ghetto riots. Now that the riots have subsided, the government is more and more devoted to gathering intelligence on campus disorder, antiwar activity and militant left and right-wing groups.

The government's justification for such surveillance is its need to be aware of potential violence, but thousands of persons are drawn in whose activities are peaceful and lawful.

For example, the Army continues to maintain a microfilm file that reportedly contains information on such persons as Mrs. Martin Luther King Jr., Georgia State Rep. Ju-

lian Bond and retired Adm. Arnold E. True, a critic of the Vietnam war.

The Army file is primarily, made up of FBI reports, and FBI reports are also the chief source of data feeding the Justice Department's computer. The FBI makes it a point to keep its information in "raw" form—unevaluated as to truth or falsity.

Those who process the FBI data at Justice say it is impossible to tell whether or not any of it comes from wiretaps. Atty. Gen. John Mitchell has declared that taps may be used without court permission on domestic organizations believed seeking to "attack and subvert the government."

Besides input from the FBI Justice's computer contains information supplied by 93 U.S. attorneys around the country and by other government agencies, such as the Treasury department's Alcohol and Tobacco Tax Division, which enforces federal firearms laws.

Some information comes also from the Secret Service, which has lately begun assembling a data bank of its own. The service's primary concern is with threats to the President, but its data bank will also contain information on demonstrations, "abusive statements" and plans to embarrass government officials.

Each week, the Justice Department computer disgorges its intelligence onto printout paper. The product is four books, each about two inches thick and enclosed in brown cardboard covers.

Each book refers to a region of the country. It contains a city-by-city assessment of the potential for civil disorder indicating what marches, rallies or meetings are occurring, the organizations and individuals sponsoring them and the city's disturbance history.

The books are combed by officials of the department's interdivisional information unit, which sends pertinent data to the attorney general and the various divisions of the department.

The community relations service gets information, for example, on potential racial problems for it to try to conciliate. The civil rights division gets reports on possible violations of the laws it enforces. The criminal division gets data on such violations as interstate movement to incite riots.

Besides city print-outs, the computer can produce a run-down on a specific upcoming major event, listing all stored information on the individuals and organizations who are planning it.

This was done, for example, prior to the Nov. 15 antiwar march on Washington organized by the New Mobilization Committee to End the War in Vietnam and the Vietnam Moratorium Committee.

Special print-out reports have also been done on at least one organization, the Black Panther Party.

Whether special reports have been prepared on individuals is not known, although interdivisional information unit director James F. Devine said it could be done if needed.

Devine, also chief of the department's civil disturbance group, declined to identify any individual whose name is on computer tape.

He said, however, that it is "impossible not to have information on nonviolent individuals." He added, "I think it's realistic to expect that what would normally be in the files of the Justice department would reflect itself in the computer. You can make your own assumptions (about who is listed). It should not be difficult."

Another Justice department official said that a specific unput report on an individual might tell "he made a speech on such-and-such a night at such-and-such a place. This is what he said. This was the result."

Government officials differ on whether computerized storage of political information is dangerous to the civil liberties of Americans.

Devine contended that it is not. He said it is "a ghost" to see danger.

"The information is here anyway, in the records of the department. Putting it on a computer is just a matter of systematizing it and making it more retrievable," he said.

He added: "Having your name on a computer does not involve the question of guilt or innocence."

This is not the attitude of the two chief congressional defenders of the right to privacy, Sen. Sam Ervin, (D-N.C.) and Rep. Cornelius Gallagher, D-N.J.

The two were responsible, along with 18 other congressmen who wrote letters, forcing the Army to abandon its political computer at Fort Holabird in Baltimore. Ervin and Gallagher are continuing inquiries into other Army political files.

Neither has commented about the Justice Department computer. It is not known whether they are even aware of its existence, for no specific authorization was sought from Congress to set it up. Justice does not believe legislation was necessary to computerize files already maintained in the department.

ADDITIONAL STATEMENTS OF SENATORS

PRISONERS OF WAR STILL A MATTER OF PRIORITY

Mr. BAKER. Mr. President, as we return to do the work of the people after the Labor Day recess I would call attention once again to one of the great unsolved problems of the year—the plight of the Americans held prisoner by the North Vietnamese.

The Communist regime remains adamant against abiding by the Geneva Convention on Prisoners to which it is a signatory power. Those agreements provide the bare minimum of guarantees for the captured men. They are entitled to health care, an adequate diet, proper shelter, and at least minimal communications with their families. In addition the government is required to notify our Government of their capture, listing their names and condition when captured.

The North Vietnamese have abided by none of these agreements.

It must remain a matter of top priority with the Government of the United States to ease the lot of these men and to continue every possible avenue of negotiation for their safe return to their waiting families.

EVERY DAY THE STAKES GROW HIGHER FOR HUMAN RIGHTS: THE LEGACY OF ROBERT F. KENNEDY

Mr. PROXMIRE. Mr. President, the past few days have been fraught with senseless violence and bloodshed, both here and abroad. The tragic bombing at the University of Wisconsin and the terrorism so prevalent in the Middle East made me think back to a speech of the late Senator Kennedy that is memorable in its insight and compassion. In his speech at Fordham University and also to students in South Africa in 1967, Senator Kennedy spoke poignantly of what must come close to being his personal philosophy:

Each time a man stands up for an ideal, or acts to improve the lot of others, or strikes out against injustice, he sends forth a tiny ripple of hope, and crossing each other from a million different centers of energy and daring, those ripples build a current that can sweep down the mightiest walls of oppression and resistance.

Mr. President, a little more than 3 years ago, Robert Kennedy spoke of political courage in the quest for human rights. It was his firm conviction, both in his words and his acts, that "only those who dare to fail greatly can ever achieve greatly."

I ask unanimous consent that this stirring and provocative statement by one of the most gifted leaders of our time be printed in the RECORD.

There being no objection, the statement was ordered to be printed in the RECORD, as follows:

THE WORK OF OUR HANDS

If you fly in a plane over Europe, toward Africa or Asia, in a few hours you will cross over oceans and countries that have been a crucible of human history. In minutes you will trace the migration of men over thousands of years; seconds, the briefest glimpse, and you will pass battlefields on which millions of men once struggled and died. You will see no national boundaries, no vast gulfs or high walls dividing people from people; only nature and the works of man—homes and factories and farms—everywhere reflecting man's common effort to enrich his life. Everywhere new technology and communications bring men and nations closer together, the concerns of one more and more becoming the concerns of all. And our new closeness is stripping away the false masks, the illusion of difference that is at the root of injustice and hate and war. Only earthbound man still clings to the dark and poisoning superstition that his world is bounded by the nearest hill, his universe ended at river shore, his common humanity enclosed in the tight circle of those who share his town and views and the color of his skin.

Each nation has different obstacles and different goals, shaped by the vagaries of history and experience. Yet as I talk to young people around the world I am impressed not by the diversity but by the closeness of their goals, their desires and concerns and hope for the future. There is discrimination in New York, apartheid in South Africa and serfdom in the mountains of Peru. People starve in the streets of India; intellectuals go to jail in Russia; thousands are slaughtered in Indonesia; wealth is lavished on armaments everywhere. There are differing evils, but they are the common works of man. They reflect the imperfection of human justice, the inadequacy of human compassion, the defectiveness of our sensibility toward the sufferings of our fellows; they mark the limit of our ability to use knowledge for the well-being of others. And therefore, they call upon common qualities of conscience and of indignation, a shared determination to wipe away the unnecessary sufferings of our fellow human beings at home and around the world.

TO RELY ON YOUTH

Our answer is the world's hope; it is to rely on youth—not a time of life but a state of mind, a temper of the will, a quality of the imagination, a predominance of courage over timidity, of the appetite for adventure over the love of ease. The cruelties and obstacles of this swiftly changing planet will not yield to obsolete dogmas and outworn slogans. It cannot be moved by those who cling to a present that is already dying, who prefer the illusion of security to the excitement and danger that come with even the most peaceful progress. It is a revolutionary world we live in; and this generation, at home and around the world, has had thrust upon it